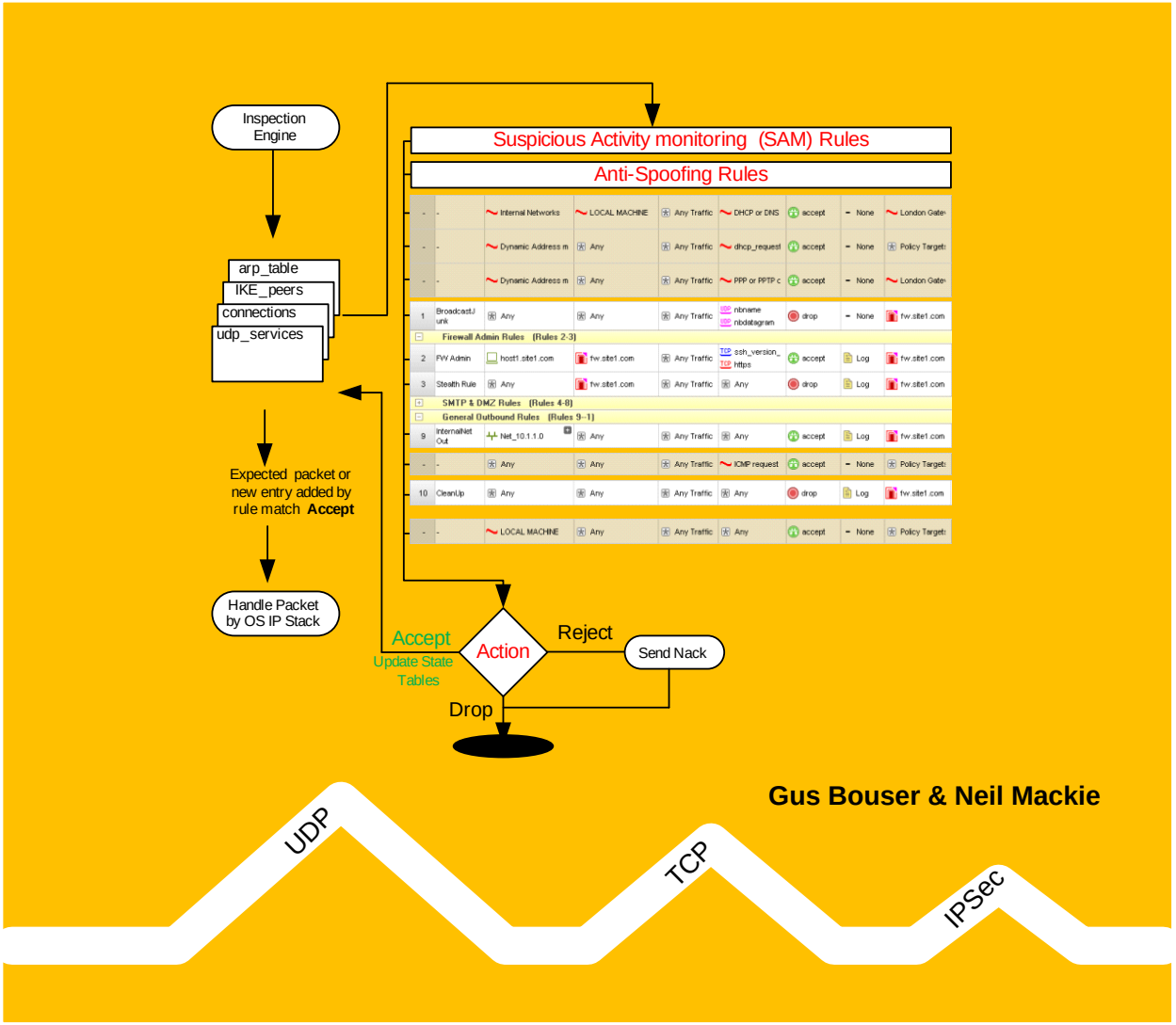
Check Point R75
Management Essentials - Part 1

Training course materials
Preparation for CCSA Certification



Printed and distributed under license from Lezha Publications by ITSec Solutions Ltd.

www.elearncheckpoint.com

6 - Creating Network Objects

Objectives

- Understand the type of objects that can be used in a Security Policy
- Create the Firewall object and change some parameters
- Establish trust between the SmartCenter and Firewall
- Understand how to set Anti-spoofing
- Know how to set the maximum concurrent connections through the Firewall
- Know how to break and reset Secure Internal communications (SIC) between a SmartCenter and Firewall
- Create the basic objects required for the classroom environment

Prerequisites

- Complete Module 5
- Virtual machines Host1, mgmt-Site1 & fw-Site1 must be running

Approximate time for completing each section

Section 1	Object Types	15 Minutes
Section 2	Creating the Firewall Object	15 Minutes
Section 3	Breaking SmartCenter & Firewall SIC	15 Minutes
Section 3	Creating General Network Objects	25 Minutes
	Total time	70 Minutes

Contents

1 Object Types

This section is background information you can select the options as you read through it but do not create any objects yet.

1.1 Object Types

Security Policy rules are created using objects.

There are some objects that are already created like TCP/UDP service definitions (lots of them) and the dynamic network objects.

All network objects you intend to use in the security policy will need to be created.

Objects can be created before you try and use them in a policy or they can be created on the fly when you realize the object is required.

Object types can be

- Network Objects
- Services
- Resources
- Servers and OPSEC Applications
- Users
- VPN Communities

1.1.1 Creating Objects

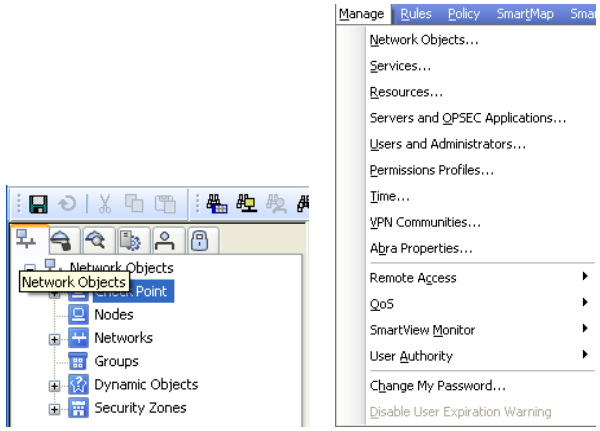
The Objects Tree has separate tabs for the different types of objects that can be created.

Each type of object has different parameters to set that may have an affect on how the security policy is enforced.

Only the most common type of network object is listed in the objects tree by default.

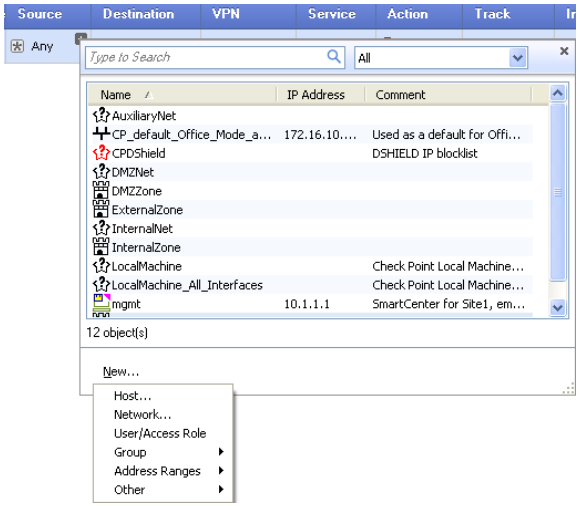
As you create an object type that is not listed by default a sub category listing will appear.

Highlighting network objects and using the 2nd mouse button will display other types of objects that can be created.



All types of objects can be created via the menu option – Manage.

If you need to create an object while editing a rule you can do this via the plus symbol in the rule element column.



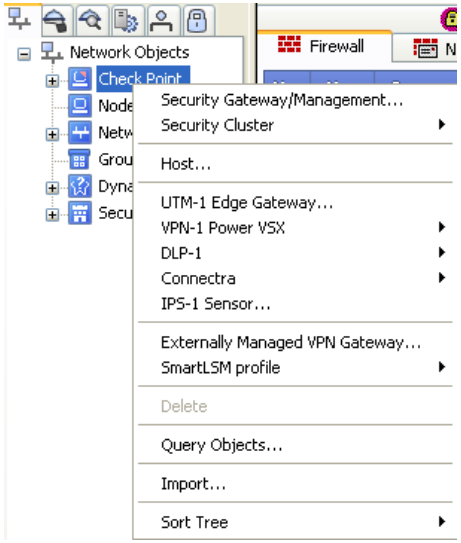
You can either add an existing object to the rule or create a new object that will then be added to the rule.

1.2 Network Objects

1.2.1 Check Point

Network objects of type ‘Check Point’ are used for objects that have a Check Point component installed and will require a license.

Check Point objects are usually gateways with multiple interfaces but do not have to be.



Check Point Object Types	
Security Gateway/Management…	Most common Check Point object created, firewall with multiple interfaces.
Security cluster	Cluster object made up of one or more firewalls, usually two firewalls.*
Host…	Usually the SmartCenter but can be a Log Server or a firewalled with a single interface, like a public web server with check Point installed.
UTM-1 Edge Gateway…	Small office appliance that can be independently managed via a web interface or integrated into the SmartCenter security policy. Admin via https://edgebox:981
VPN-1 Power VSX	Virtual firewalls, allows multiple independent firewalls to be run on a single hardware device. Often used in very large enterprises or hosted firewall service in datacenters.
DLP-1	Data Loss Prevention. This can be a Blade on a firewall gateway or a standalone appliance. Scans SMTP, FTP and HTTP traffic for data being sent out of the enterprise.
Connectra	SSL VPN gateway. Can be a Blade on a firewall gateway or a standalone appliance.
IPS Sensor…	An appliance that can be a gateway or inline inspection device. Effectively implements the IPS features of the IPS Blade, cheaper than a full firewall. ‘InterSpect Gateway’ back in NG.
Externally Managed VPN Gateway…	Used when creating VPNs when you know the partner has a Check Point gateway. If you don’t know the VPN endpoint vendor appliance use object type ‘Interoperable device’.
SmartLSM profile	Define profiles that are used as part of SmartProvisioning for deploying standard profiles on gateways.

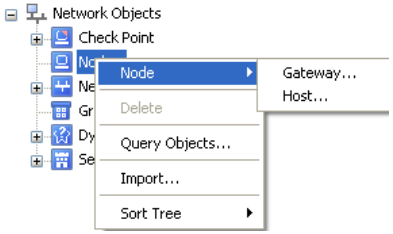
*You would only create a cluster with one firewall if you knew that in the future you were going to add a second gateway for High availability.

It is much easier to just add the second gateway than create a cluster from an existing firewall with VPNs configured for it.

All VPNs will break and need to be deleted and recreated when migrating from a single gateway to a clustered gateway configuration.

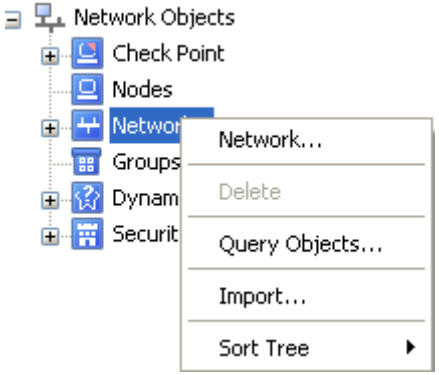
1.2.2 Nodes

Node objects are either Gateway or Host, usually host.
Examples are FTP, Web and SMTP servers.
They are named objects with an IP address.



1.2.3 Network

Network objects are just network address and subnet mask.



You may have multiple networks for example

10.1.0.0/24
10.1.1.0/24
10.1.2.0/24
10.1.3.0/24

You can also use a single object in the SmartCenter to represent all of them.

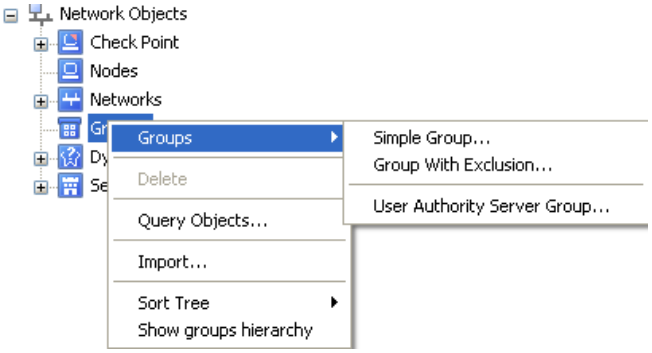
10.1.0.0/255.255.252.0

You may need to define individual network objects for each one depending on the rules for the security policy.

Check Point requires the full netmask to be defined not the shorthand / format.

1.2.4 Groups

Group objects are used extensively in Check Point and you can use nested groups, groups within groups.



1.2.5 Dynamic

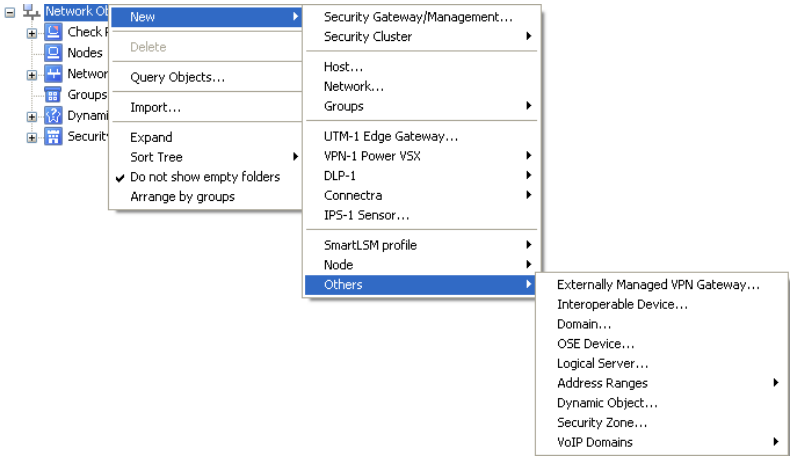
A dynamic object is a logical object where the IP address is resolved differently per Check Point Security Gateway using the dynamic_objects command.

1.2.6 Security Zones

A Security one is a logical network object that represents interfaces with a common security policy. Used for UTM-1 Edge devices for small offices.

1.2.7 Others

The ‘Others’ type of objects are not listed by default and will only appear in the Object Tree once you create an instance of that object type.



Other Object types

Interoperable Device…	Used for defining partner VPN endpoints.
Domain…	DNS domain object.
OSE Device…	Third party router devices that can have security policies generated and installed from the SmartCenter.
	Requires optional license.
Logical Server…	Used for Connect Control Load balancing module. Optional license required.
Address Ranges	Network address range for IP addresses, 1.1.1.1 to 1.1.1.30
VoIP Domains	Objects for VoIP protocols, SIP, H.323, MGCP, SCCP

1.2.8 VoIP Domains

Check Point has added extensive INSPECT checking for VoIP protocols and requires careful setup of the correct type of object and service in a rule to enable VoIP protocols to work through a Check Point firewall.

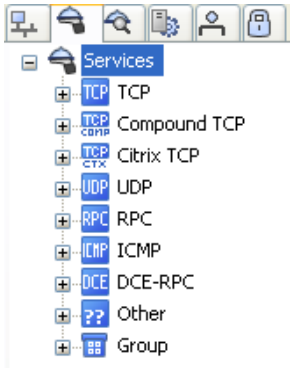
VOIP protocols tend to use a large number of dynamically allocated ports and can tunnel video and data that makes them difficult to secure.

The implementation of VOIP protocols by software vendors is relatively new and the interpretation of an RFC by developers and security implementers are not always the same.

1.3 Services, Resources, OPSEC, Users & VPN Communities

1.3.1 Services

The services tab lists a large number of predefined objects that can be used in the Services column of a rule.



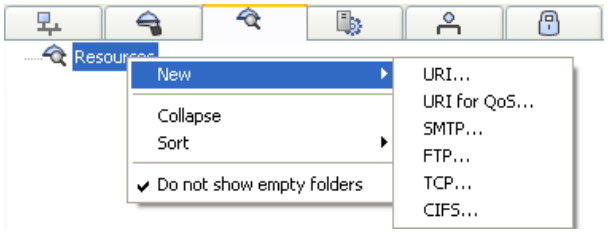
Note: Just because a service is predefined does not mean that the Check Point inspection engine will filter at the session/data level for that protocol. It may just be looking at the port number.

INSPECT code has been added for lots of services to filter at the Session/Data level. However, the only way to be sure is to try and abuse the protocol to see if you can effectively tunnel anything over it. This applies to all firewalls not just Check Point.

Abusing a protocol and tunneling a different application over it is demonstrated later. The example is not sophisticated and requires only simple networking knowledge.

1.3.2 Resources

Resources relate to the Content Security Servers, usually limited to a few services, HTTP, FTP, and SMTP.
There is also a generic TCP resource for handing data streams to external virus content scanners.



Large enterprises are likely to use a dedicated application content security appliance like Bluecoat, Websense, MailMarshal,MimeSweeper to handle detailed inspection of http, ftp, smtp data streams.

Not everyone has the budget for these appliances. The use of Resources can fill a security gap and should not be ignored. Resources are explained later.

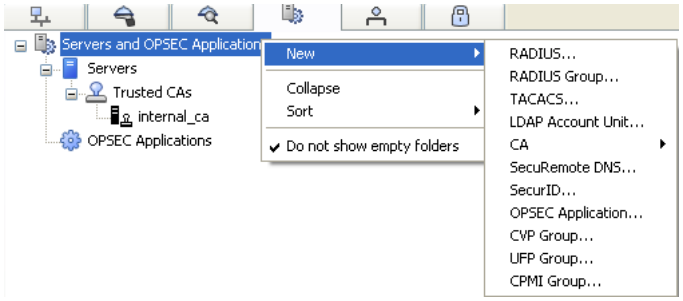
1.3.3 Servers & OPSEC Applications

These object types have predefined characteristics, for example RADIUS or Certificate Authority servers.

OPSEC - Open Platform for Security Enterprise Connectivity.

This is Check Points platform for third party vendors to certify their products as Check Point compatible.

A list of different products that have been certified is available at www.opec.com.



The ‘internal_ca’ object is automatically created when the SmartCenter is installed.

It is responsible for signing all certificates generated by the SmartCenter for use by firewalls.

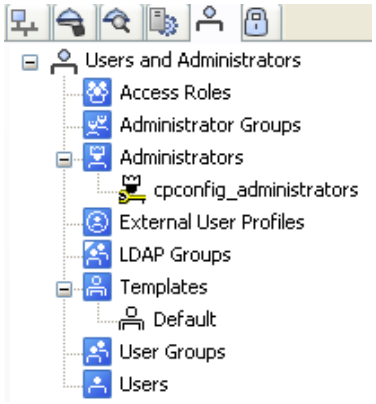
If this object is corrupted VPN communications will break.

1.3.4 Users and Administrators

There are two types of users.

Administrators	Used for logging into the SmartCenter to control the Security policies. The first administrator is managed by 'cpconfig' all others are created and edited in the SmartDashboard.
General Users	Used for matching a user when required by a rule in a security policy.

General Users must belong to a Group to enable a match in a rule.



External authentication databases can also be integrated into the security policy.

An example would be using RADIUS or LDAP where the firewall hands the request for authentication off to an external server and does not hold the user details in a local firewall database.

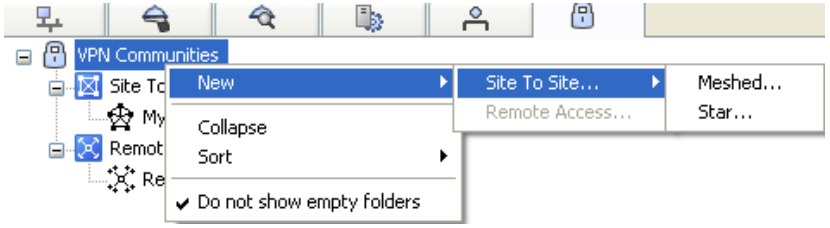
Using an External database can simplify user account management.

1.3.5 VPN Communities

VPN communities allow a relatively simple method of defining encryption parameters within the SmartDashboard.

The Site to Site communities are for gateway to gateway encryption supporting any IKE/IPSec compliant gateways.

The Remote Access community is for use with Check Point's SecureClient desktop application for securing remote users using IKE/IPSec.



Site to Site Communities can be either Mesh or Star (Hub) based.

Mesh based communities allow all of the members to directly connect to each other.

Star based communities allow all the members to communicate only via a central hub.

2 Creating the Firewall Object

2.1 Check Point Gateway Object

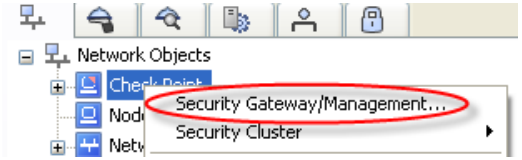
A SmartCenter license has a limited number of firewall modules it can manage unless it is an unlimited license.

In a live environment you will need a SmartCenter license that can manage the number of firewall modules you have deployed.

For example, a three site SmartCenter license can manage up to three firewall modules.

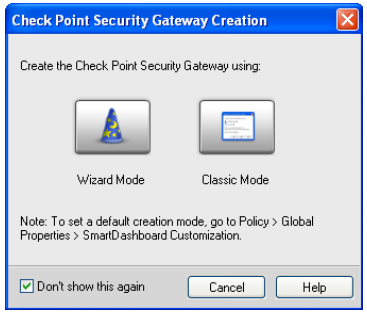
A separate license is required for each firewall module.

2.1.1 Create a New Check Point Gateway

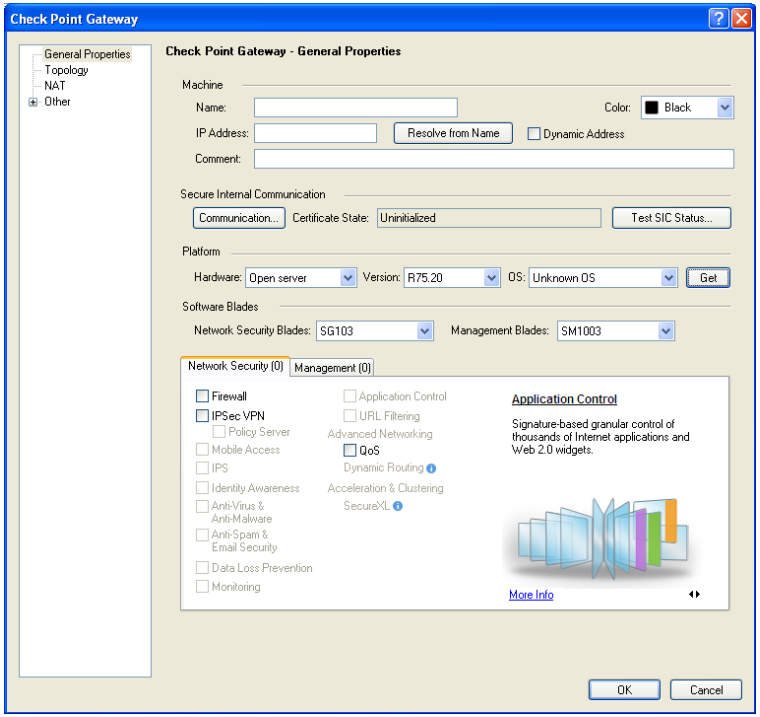


There is a wizard option for creating the firewall object but it is easier to just set all the values from the main dialog.

Select 'Don't show the dialog again' and 'Classic Mode'

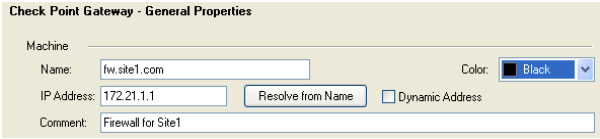


The list of tabs on the left may change depending on what blades are selected. At the moment there is no VPN tab as it's not required since 'IPsec VPN' is not selected.



2.1.2 Set the Hostname and IP address 172.21.1.1

Fill in the Name, IP Address, and Comment.



The IP address should be the external address although in some cases it may have to be the internal address. If you have a single firewall (not clustered) then the external address should always be used.

The IP address defined in the general properties will be the address that is used as the VPN endpoint address by default.

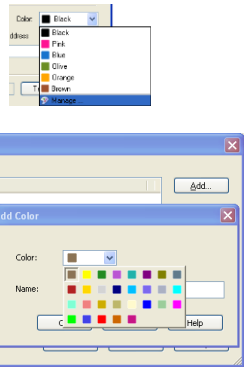
The SmartCenter will always try and connect to the IP address defined in the general tab when it installs policies. That can sometimes be a problem when using clusters.

If you manage UTM-1 Edge devices from the SmartCenter and create VPNs between them and a gateway has an internal IP address in the general tab set you may have problems.
The Edge device might try and use the internal address as the tunnel endpoint which it cannot do over the internet. It was a bug and may have been fixed depending on the firmware installed on the UTM-1 Edge device.

2.1.3 Set the Color to Red

Check point removed the large selection of colors that used to be available in previous versions and you need to add colors to the selection list if you want to use them.

Set the color to Red

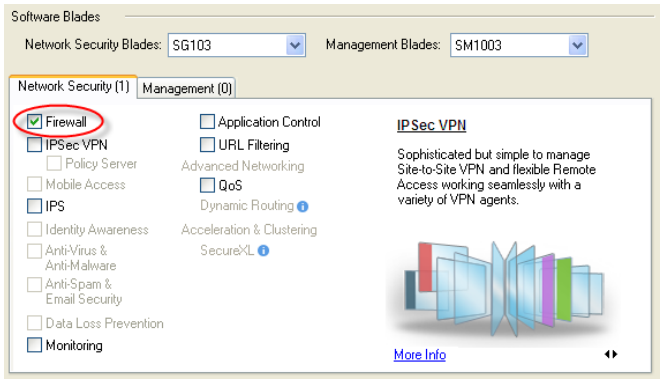


It is fairly common to try and set a color code standard for object types. Usually doesn't last very long but always good to make an effort.

2.1.4 Select Check Point Software Blades

For the moment the only Check Point product that needs to be selected is the Firewall.

Select the Firewall Blade



Some of the other Blades will be turned on later when required.

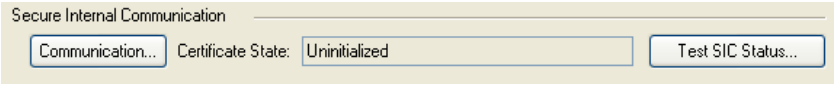
In live environments you need the right license to be able to turn on the Blade. This is an evaluation environment so everything will work.

You can normally select a blade to turn it on even if you do not have a license for it. When you try and install the policy if you do not have a license then the policy will not install.

2.1.5 Set Secure Internal Communications

Setting communications will establish a link with the firewall and establish trust so that the firewall can be controlled from this SmartCenter.

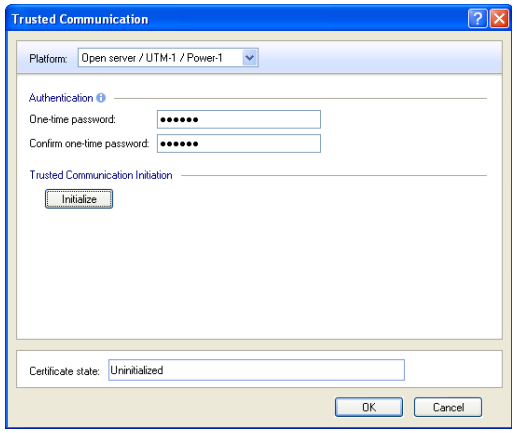
At the moment the firewall is not under the control of any SmartCenter.



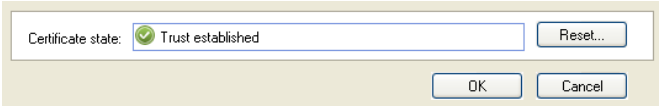
Select Communication

Enter the Shared secret – abc123

This is a one time secret to authenticate the self signed Diffie Hellman public key that will be exchanged between the firewall and SmartCenter.



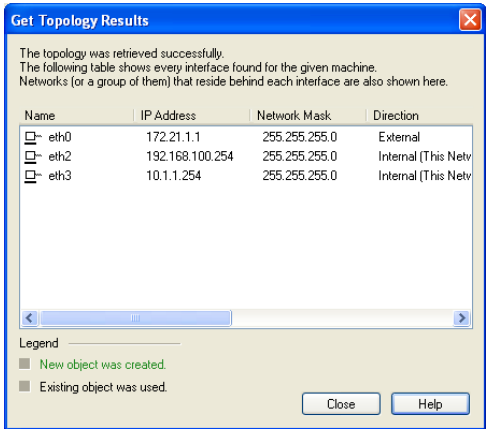
Select Initialize



The Trust state should change to '**Trust established'**.

Select OK

The topology information is automatically fetched from the firewall. This is the IP address and networks associated with each interface. The topology tab is where anti-spoofing is configed.



If you get '**Initialized but trust not established**' then it could be

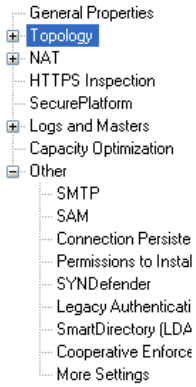
- SmartCenter cannot connect to the firewall module. Likely to be an IP address or routing issue.
- The shared secret is incorrect. You need to reset SIC on the firewall module and select 'Initialize' again.
- The virtual machine network interface in not connected.
- The virtual machine Ethernet setting is on the wrong virtual network, VMnet0, VMnet1, VMnet2, through VMnet9. Each is a separate VLAN. Make sure the same networks are connected to the same VMnet.

The virtual machine issues only apply to this training environment.

Providing you have established trust then you can move onto the next step. If not you must debug the problem first.

2.1.6 Changes to the Firewall Tab Option List

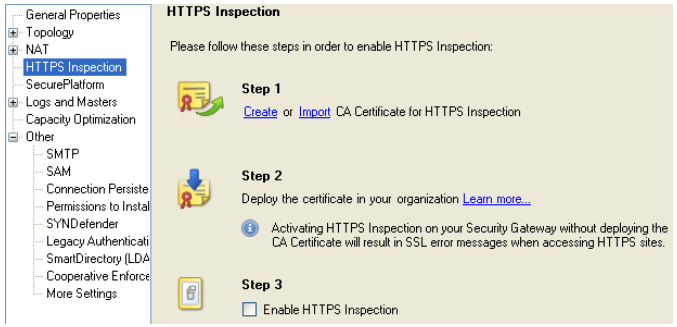
Extra options have been added to the Tab list because this object has a Firewall Blade installed on it.



2.1.7 HTTPS Inspection

This is one reason never to trust using HTTPs from a corporate environment.

No change required



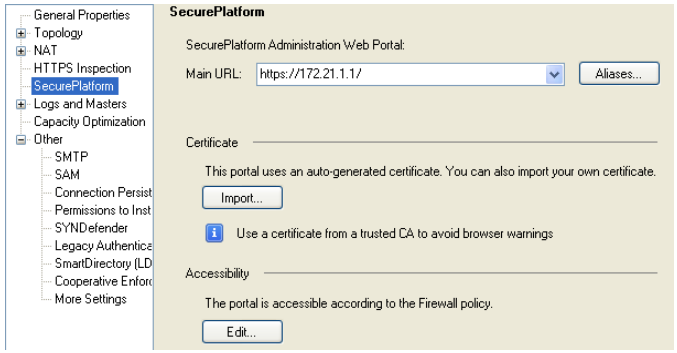
HTTPS is usually a client to sever endpoint encryption. However, it is possible to deliberately build a Man in the Middle gateway that allows full content inspection.

Effectively breaks the trust of SSL connections.

The simple rule is DO NOT USE HTTPS Internet banking from work or an unknown computer.

2.1.8 SecurePlatform

No change required.

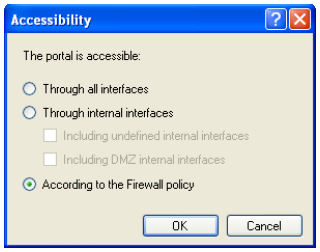


The SSL connection to the WebUI for SPLAT uses a self signed certificate which will produce certificate errors.

It is possible to import a certificate from an external trusted CA to remove the warning.

Accessibility to the WebUI is usually controlled by adding rules to the Security policy to explicitly allow access if required.

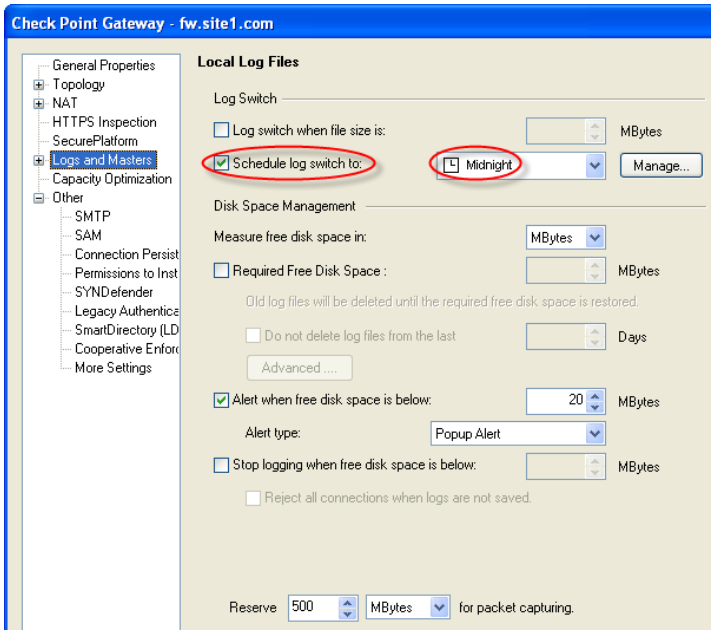
This can be overridden, not usually done!



2.1.9 Setting Logs And Masters

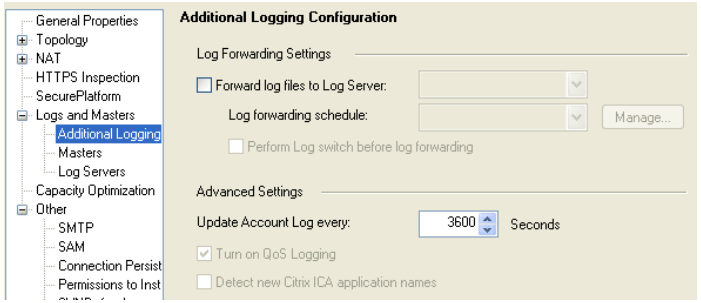
The firewall will only log to its local disk if it is specifically set to log locally or the firewall has lost connectivity to the SmartCenter.

Turn on log rotation to occur at Midnight.



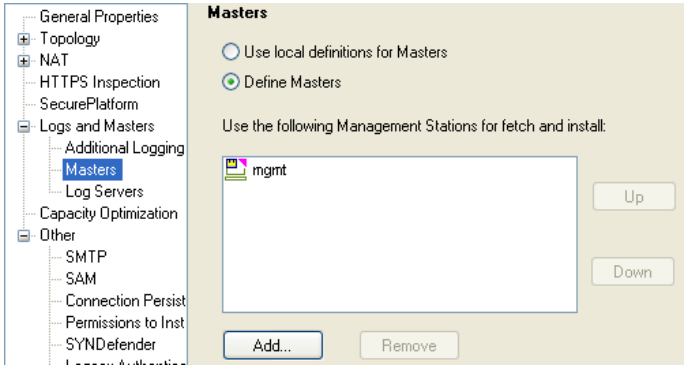
There is an option to forward the log files to another Log Server. A SmartCenter is bundled with a Log Server by default but you can purchase a separate license that will just be a Log Server.

No change required.



The Masters tab lists the SmartCenters that are allowed to install security policies on this gateway.

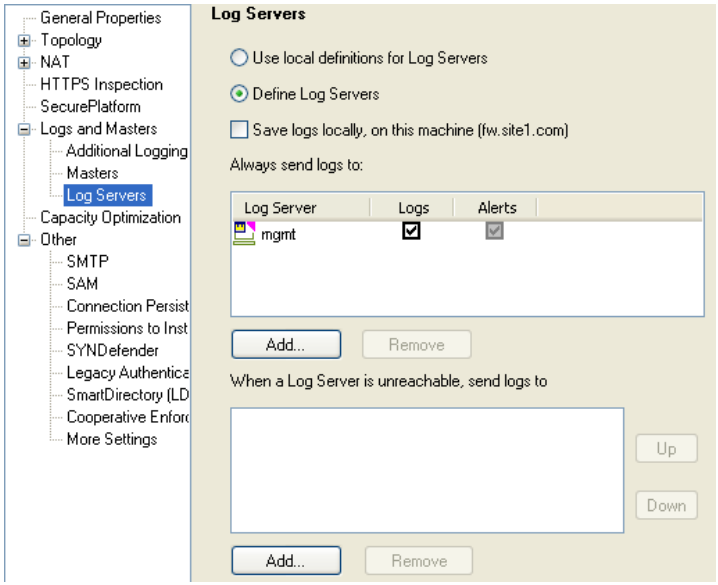
No change required.



The Log Server tab allows you to explicitly set where the firewall will send logs.

If you have a large firewall deployment you may have purchased a separate log server and moved the logging from the SmartCenter to a dedicated log server with a large storage capacity.

No change required.



Logs file size can grow very quickly and should be monitored.

Settings are available to generate alerts when thresholds are met and should be configured in a live environment.

Log threshold alerts should be set on both the Firewall and SmartCenter objects.

2.1.10 Capacity Optimization

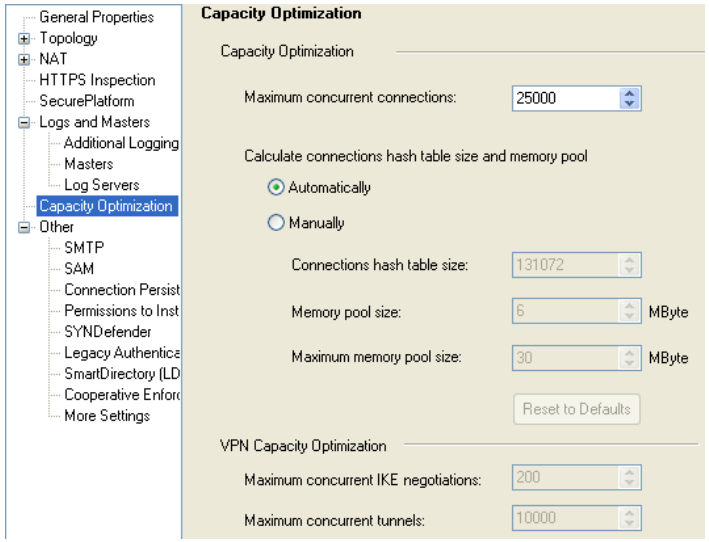
This determines the number of connections that the firewall will be able to handle.

Just because you can set the value to 100,000 does not mean you should.

You would need an appropriate server with enough CPU & memory resources.

The default value is 25,000 connections.

No change is required.

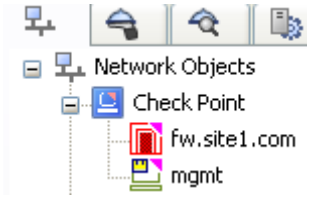


The other options will be introduced later.

You should now have a good overview of the parameters that can be set on a firewall object.

Select 'OK' to finish creating the firewall object fw.site1.com.

You should now have two Check point objects listed in the Objects List.



The following commands will display helpful information regarding firewall connections and memory use.

```
fw ctl pstat

fw tab -t connections -s
```

3 Breaking SmartCenter and Firewall Communications

3.1 Breaking and Resetting SIC

There will be times when you need to reset Secure Internal communications (SIC) between a firewall module and the SmartCenter.

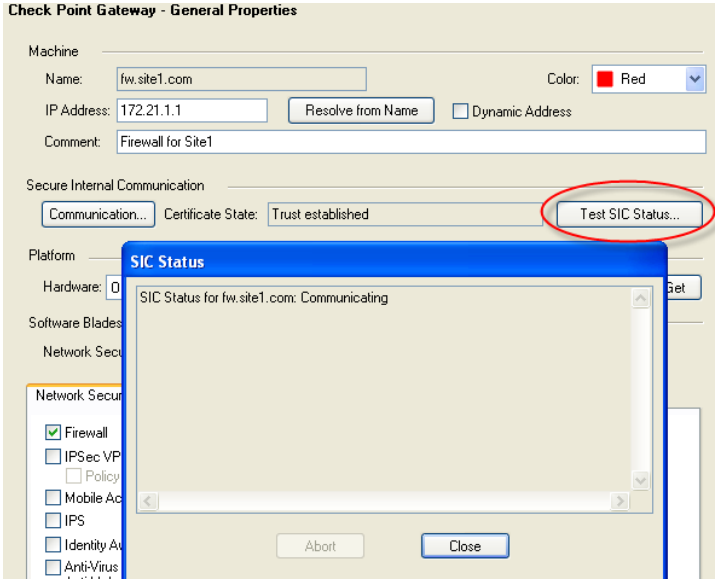
If communications break you will need to reset SIC in two places

- On the Firewall using ‘cpconfig’
- The firewall object.In SmartDashBoard,

When you reset SIC the policy on the firewall will revert to ‘InitialPolicy’.

On a live system this may be an issue since no traffic is routed via the firewall and network downtime will occur.

Test SIC before you stat



3.1.1 Reset SIC on the Firewall

To reset SIC on the firewall, login to the firewall and run ‘cpconfig’.

Login using either the console or SecureShell.

```
Check Point SecurePlatform R75.20
For Web User Interface access connect to https://172.21.1.1

login: admin
Password:
Last login: Mon Mar 26 14:30:38 on ttyS0

? for list of commands
sysconfig for system and products configuration

[fw]# fw stat
HOST       POLICY     DATE
localhost InitialPolicy 26Mar2012 14:29:37 :  [>eth0] [>eth3]
```

Run cpconfig

```
[fw]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  SNMP Extension
(3)  PKCS#11 Token
(4)  Random Pool
(5)  Secure Internal Communication
(6)  Enable cluster membership for this gateway
(7)  Automatic start of Check Point Products

(8) Exit

Enter your choice (1-8) : 5
```

Select option 5 to reset SIC

```
Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Trust established

Would you like re-initialize communication? (y/n) [n] ? y

Note: The Secure Internal Communication will be reset now,
and all Check Point Services will be stopped (cpstop).
```

```
No communication will be possible until you reset and
re-initialize the communication properly!
Are you sure? (y/n) [n] ? y
Enter Activation Key: abc123
Retype Activation Key: abc123
initial_module:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


The Secure Internal Communication was successfully initialized


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  SNMP Extension
(3)  PKCS#11 Token
(4)  Random Pool
(5)  Secure Internal Communication
(6)  Enable cluster membership for this gateway
(7)  Automatic start of Check Point Products

(8) Exit

Enter your choice (1-8) : 8
```

Select Option 8 to Exit

```
Thank You...
Stopping SmartView Monitor daemon ...
SmartView Monitor daemon is not running
Stopping SmartView Monitor kernel ...
Driver 0 is already down
SmartView Monitor kernel stopped
rtmstop: SmartView Monitor kernel is not loaded
FloodGate-1 is already stopped.
FireWall-1: UserCheck server is not running
VPN-1/FW-1 stopped
SVN Foundation: cpd stopped
Multiportal daemon: mpdaemon stopped
SVN Foundation: cpWatchDog stopped
SVN Foundation stopped
cpstart: Power-Up self tests passed successfully

cpstart: Starting product - SVN Foundation

SVN Foundation: Starting cpWatchDog
SVN Foundation: Starting cpd
Multiportal daemon: starting mpdaemon
SVN Foundation started

cpstart: Starting product - VPN-1

FireWall-1: starting external VPN module -- OK
FireWall-1: Starting fwd


Installing Security Policy InitialPolicy on all.all@fw
Fetching Security Policy from localhost succeeded
 Failed to read database.
 Probably module was never installed
 Failed to fetch policy from masters in masters file
FireWall-1: enabling bridge forwarding
FireWall-1 started

cpstart: Starting product - FloodGate-1

FloodGate-1 is disabled. If you wish to start the service, please run
'etmstart enable'.

cpstart: Starting product - SmartView Monitor

SmartView Monitor: Not active
cpridstop: cprid watchdog stopped
cpridstop: cprid stopped
cpridstart: Starting cprid
[1] 17413
[fw]#
```

If using SecureShell to the firewall you will likely loose connectivity and need to reconnect.

```
[fw]# fw stat
HOST      POLICY     DATE
localhost InitialPolicy 29Mar2012 19:20:22 :
[fw]#
```

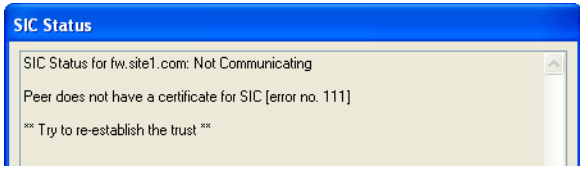
Now you need to rest SIC at the SmartCenter for the firewall object.

3.1.2 Test Trust for the Firewall Object in the SmartCenter

Trust was established earlier but since a new DH key pair and public key certificate has just been created the SmartCenter will have the wrong certificate associated with the firewall object.

Testing SIC should now fail.

Edit the Firewall Object, Communications, Test SIC



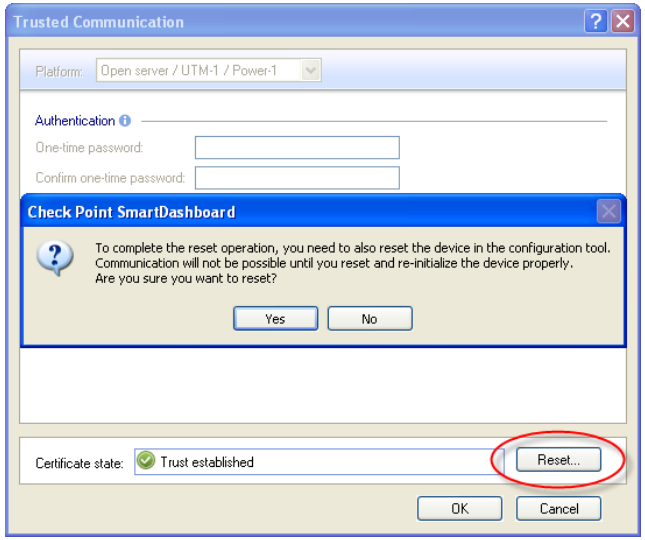
Note: Just because the SIC connectivity test fails does not always mean that SIC is broken.
It was deliberately broken here to demonstrate how to reset it.
In a live environment there could be network connectivity issues or a security policy might have been installed that prevents the SmartCenter connecting to the firewall.

3.1.3 Reset SIC in the Firewall Object

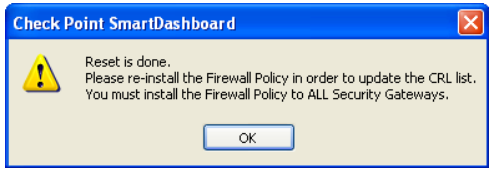
To reset SIC, edit the firewall object and select Communications, Reset.

Reset SIC on the firewall object.

There are several warnings because this is not something you want to do by mistake.

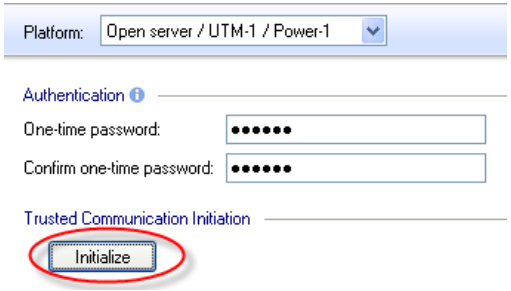


You can either do the reset on the SmartCenter first or Firewall but it will need to be completed on both locations. Usually the firewall is completed first since you will get immediate feedback to confirm trust is established if you do the SmartCenter bit second.



The reset cleared the cached DH firewall certificate and now a new connection needs to be established with the firewall.

Enter the Activation Key and Select Initialize.



Test SIC Communications again and it should now work.

Now the SmartCenter is back to being able to install policies on the firewall.

Make sure you select 'OK' to save the firewall object changes.

4 Creating General Network Objects

This next section creates typical network objects that are required for a basic security policy.

The objects mostly relate to the training environment but a few of the objects demonstrate the problems that can occur in a live environment.

Because the training environment is limited with the number of virtual machines some of the objects will not necessarily exist but will be created and used as part of the security policy.

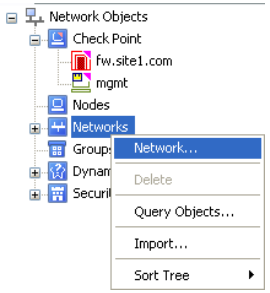
Network Address Translation will be dealt with later. Therefore, no changes will be required to the NAT tab setting for any of the objects created in this section.

4.1 Creating the Network Type Objects

Network objects are always defined with a Name, Network address and Subnet mask.

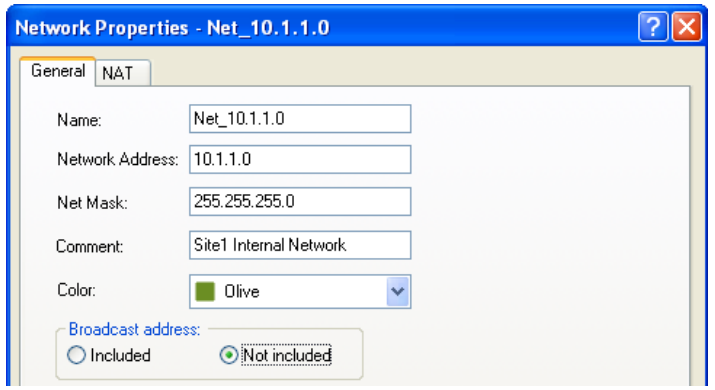
4.1.1 Create the Internal Network

Select Network from the Objects Tree –Network



Complete the Network dialog
Set the Broadcast Address to Not Included.

Name	Net_10.1.1.0
Network Address	10.1.1.0
Net Mask	255.255.255.0



Select 'OK' to create the object.

4.1.2 Network Object – Broadcast Address

In general the setting should be set to 'Not included'.

This means that when the network object is used as a source or destination in a rule the broadcast address will not be treated as part of the network and therefore will not match the rule.

If you do not set the broadcast address to 'Not Included' then it may allow the following.

A user on the internal network creates a packet that has the destination 80.1.1.1 (an external public address) with a source IP address of 10.1.1.255.

The packet is routed to the firewall and matches an outgoing rule.

The firewall has been configured with Network Address translation to change the internal network address to hide behind the external IP address of the firewall.

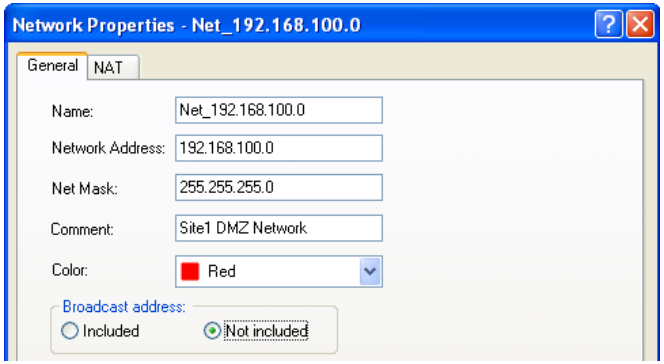
The packet is sent out with the firewall address but when it receives the reply it maps the Network Address Translation back to 10.1.1.255 and creates a broadcast storm back onto the internal network.

Send one packet out and get multiple back.

4.1.3 Create the DMZ Network

Complete the Network dialog.

Name	Net_192.168.100.0
Network Address	192.168..100.0
Net Mask	255.255.255.0



4.1.4 Create the External Network

This uses an alternative method of creating the network object. If you have SmartMap then you can use it as an interface for editing and creating network objects. The evaluation license includes the use of SmartMap.

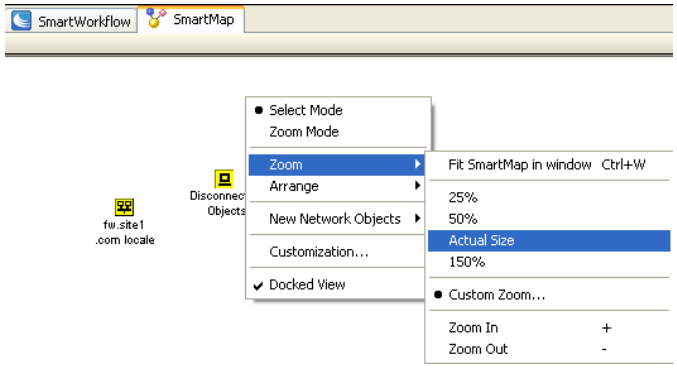
Some of the objects, like the firewall, have what are called ‘implied networks’ based on the objects interface IP addresses.

The IP address associated with an interface on the firewall will have a network and subnet mask. The network object can be created using ‘actualize’ from within SmartMap.

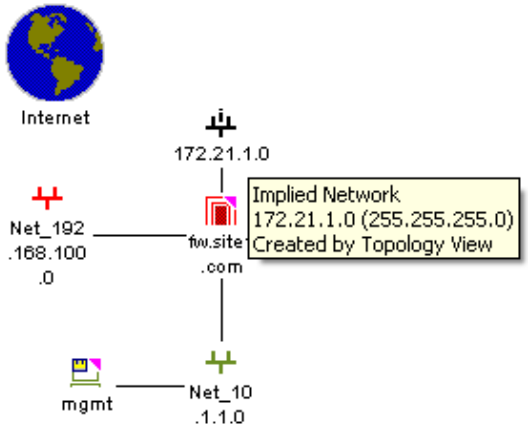
The initial layout in SmartMap may be difficult to see.

To use SmartMap it must be enabled and after it has been enabled you must logout and back into SmartDashboard.

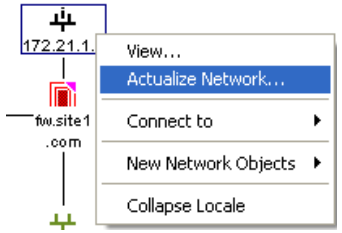
Select Zoom – Actual Size



You may have to adjust the layout slightly to keep the diagram tidy. The 172.21.1.0/24 network is an ‘Implied Network’ because the firewall has an interface IP address within the network range.

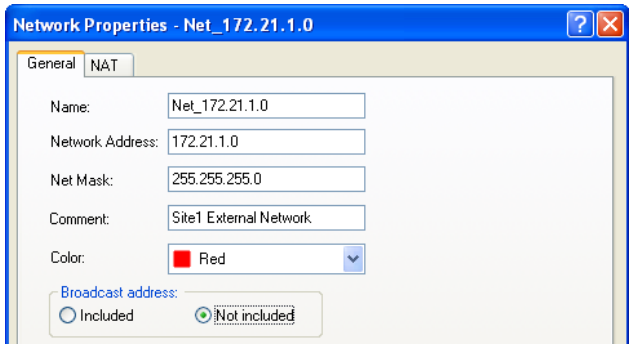


Use 2nd Mouse button and Select Actualize Network.



The network dialog is displayed with completed fields using the default naming convention **Net**_.

Complete the Network dialog, Color and Comment, Broadcast Address.

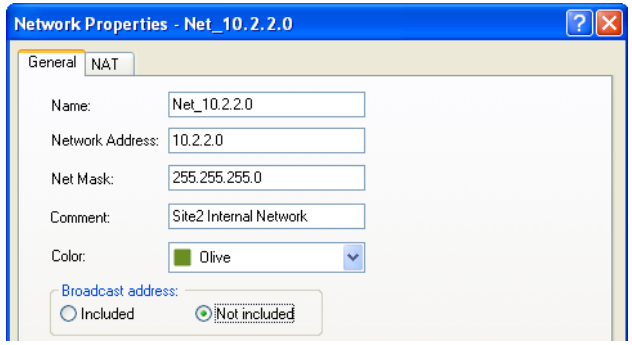


4.1.5 Create the Remote Site2 Network

This network will be used later when managing multiple firewalls.

Complete the Network dialog.

Name	Net_10.2.2.0
Network Address	10.2.2.0
Net Mask	255.255.255.0



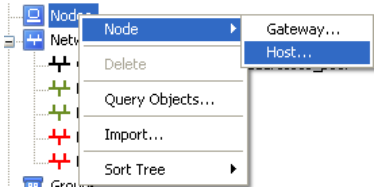
4.2 Creating Node Type Objects

Node objects can either be Hosts or a Gateway, they are usually hosts as the majority you create will only have a single IP address. You might configure the Classroom router as a Gateway object but it is not necessary.

4.2.1 Create the Internal Server adsrv01

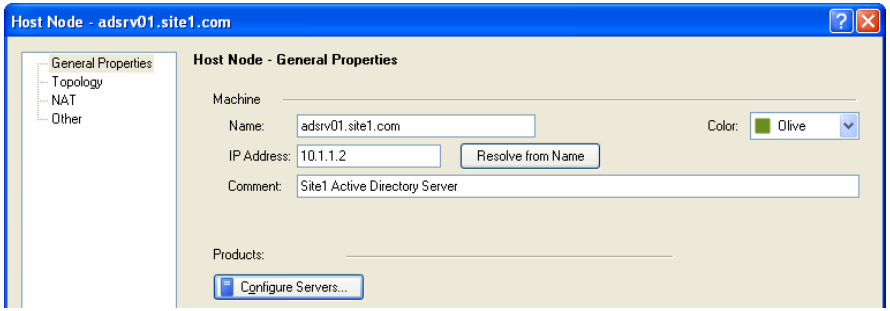
This object will act as the Active Directory server for site1. It also has an FTP and Web Server roles enabled.

Create a Node – Host object



Fill in the details for Site1 Active Directory server.

Name	adsrv01.site1.com
IP Address	10.1.1.2



A host type object can be assigned a particular role, SMTP, Web or DNS server that adds extra INPSECT checking. This is selected via the 'Configure Servers…'

Select 'OK' to create the object.