



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957

Fax: 919.217.5769

CISCO VPN 3000 INTEGRATION ISSUES

Products: Cisco VPN 3000 series VPN concentrator

Overview

The Cisco VPN 3000 series of VPN concentrators provides network administrators and engineers with a hardware platform capable of supporting a variety of VPN encryption protocols, operating systems, encryption strengths, and authentication methods. This technical document describes some specific issues that might be encountered when integrating the VPN 3000 series concentrators into a network.

More Information

PPTP Encryption and RADIUS Authentication

In order for Windows-based clients to use encryption with PPTP tunnels, MS-CHAP v1 or v2 must be used for authentication. RADIUS servers that do not support MS-CHAP v1 or v2, therefore, will not be able to support PPTP encryption on the tunnels. Anyone with a network sniffer will be able to decode the GRE (Generic Routing Encapsulation) tunneling used by PPTP and see the contents of the “private” traffic, rendering the tunnels useless with regard to security.

Internet Authentication Service (IAS), included with Windows 2000 and as part of the Option Pack for Windows NT 4.0, supports MS-CHAP and can therefore support encrypted PPTP tunnels.

SecurID Support for Authentication

The VPN 3000 series supports SecurID, from RSA Security, for authentication. SecurID offers enhanced security through the use of ever-changing passwords and security tokens. When using SecurID for authentication, however, there are some specific limitations that arise. Some of these issues are described below.

- SecurID only supports PAP authentication. Therefore, PAP authentication must be enabled for PPTP and L2TP clients. Native IPSec clients must have SecurID selected as the authentication type for their group. (While RSA Security’s ACE/Server offers a RADIUS interface to the SecurID database, this RADIUS server also only supports PAP authentication.)
- Because SecurID only supports PAP authentication, encryption on PPTP tunnels is not supported. Therefore, all PPTP tunnels will be unencrypted (and therefore insecure).

- Windows-based PPTP and L2TP clients will most likely require that PAP be activated, since PAP is typically not an active authentication method. This requires manually editing the properties of the VPN connection to enable PAP.
- Note that when using SecurID (and therefore PAP) with L2TP over IPsec tunnels, the IPsec SA is established before the username/password information is sent across the link. This alleviates potential security concerns about the unencrypted nature of PAP authentication, since the encryption in this instance is being provided by IPsec.

More detailed information regarding SecurID, its limitations, and features can be found on RSA Security's web site.

Windows 2000 L2TP over IPsec Support

Windows 2000 has built-in support for L2TP over IPsec. The VPN 3000 concentrators support L2TP over IPsec as implemented by Microsoft in Windows 2000. However, Windows 2000 clients must be configured in a very specific way in order to interoperate fully with the VPN concentrator.

- The Windows 2000 client must be configured to prohibit the automatic creation of an IPsec policy when establishing L2TP connections. This is described in greater detail in Microsoft Knowledge Base article Q258261, titled "Disabling IPSEC Policy Used with L2TP."
- Because automatic IPsec policy creation has been disabled, an IPsec policy to secure L2TP traffic (UDP port 1701) must be manually created and activated. This policy must specify security parameters that match those on the VPN concentrator. The technical document titled "Using L2TP Over IPsec from Windows 2000 to a Cisco VPN 3000" provides more information on the details of the IPsec policy required to support L2TP over IPsec.
- All Windows 2000 clients must have digital certificates from a compatible certificate authority. The OU field from this digital certificate must match the OU field from the digital certificate on the VPN concentrator. (Windows 2000's Certificate Authority is supported.)

In addition, there are some specific configuration steps that must be taken on the VPN concentrator as well. These configuration steps are described below.

- The VPN concentrator must have a digital certificate from a compatible certificate authority. In addition, the OU field on this digital certificate must match the OU field on the digital certificates installed on the Windows 2000 clients.
- The VPN concentrator must have a group defined that matches the OU field on the digital certificates. The password for this group is irrelevant.
- The VPN concentrator must have an active IKE proposal that matches the IPsec configuration on the Windows 2000 clients (IKE-3DES-MD5-RSA is the recommended IKE proposal).
- The ESP-TRANSPORT-L2TP IPsec SA must be modified to use the digital certificate for authentication. (It may be best to create a new IPsec SA and set the parameters manually to match those in ESP-TRANSPORT-L2TP.)

More detailed information can be obtained from Cisco's web site.

OSPF in LAN-to-LAN Connections

Currently, IPsec does not have any method for handling multicast or broadcast traffic. As a result, routing protocols such as OSPF will not travel across IPsec-based LAN-to-LAN tunnels. The VPN concentrator can learn routes from interior routers via OSPF, but will not be able to pass those routes across VPN tunnels via OSPF.

It may be possible to redistribute OSPF routing updates into RIP, then allow VPN concentrators to use RIP to pass information between them. RIP updates received by the VPN concentrator can then be redistributed back into OSPF. However, this has not been tested in a real-world implementation.

LAN-to-LAN Tunnels with PIX Firewalls

The VPN 3000 series of concentrators is fully capable of supporting 3DES-encrypted IPsec VPN tunnels to PIX firewalls with a 3DES VPN license. However, real-world implementations of this type of configuration have shown that if network connectivity to the VPN 3000 is lost or interrupted, the VPN tunnel between the concentrator and the firewall will not re-establish itself automatically due to a live IPsec SA (security association) on the firewall (i.e., the firewall thinks the tunnel is still “up”). To resolve this issue, the `clear ipsec sa` and `clear isakmp sa` commands must be issued on the PIX firewall while in configuration mode.

Other Notes

None

Related Articles/Resources

Additional information on SecurID can be found at RSA’s web site (<http://www.rsasecurity.com>).

Cisco Connection Online (CCO), Cisco’s web site, also has additional information on the VPN 3000 series of VPN concentrators. CCO is found at <http://www.cisco.com>.

In addition, the following Microsoft Knowledge Base article provides additional information on the necessary IPsec policy changes required to support Windows 2000-based L2TP over IPsec connections:

Q258261: Disabling IPSEC Policy Used with L2TP

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.