

PROCEDURE 1410.22
Issued: March 15, 2001
Effective Date: March 15, 2001

SUBJECT: External Gateway to Home Gateway, Multi-Node
Virtual Private Network (VPN)

APPLICATION: Executive Branch Departments and sub-units and non-executive branch entities when accessing the State of Michigan (SOM) data communication networks and hosts from external public, partner, or any non-trusted networks using the Internet Protocol suite (TCP/IP).

PURPOSE: To standardize a gateway to gateway (multi-client or multi-host node or mixed client and host) VPN security policy and guideline for State of Michigan agencies connecting to internal data communications networks from locations over host networks not controlled, operated, or managed by or for the State of Michigan. A policy-determined level of cooperation must exist with the management team on the remote host network related to firewall-rules, gateway configurations, and access control lists for this standard to operate.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Strategic Policy

TELEPHONE: 517/373-7326

FAX: 517/335-2355

SUMMARY:

This procedure establishes **IPSec** as the gateway peer to gateway peer technology adhered to in compliance with the State of Michigan security policy and best practice to protect internal networks, devices, and hosts from external security threats posed by transmitting data requiring protection over the Internet or other external network.

The **IPSec** structure provides origin authentication, integrity, confidentiality through encryption, and anti-replay security services. Personnel authentication, where required, will be achieved using enterprise approved two-factor authentication (currently Securid card).

The inclusive transport mechanisms and international standard protocols include:

TCP/IPv4 v6, L2TP, IPSec, ESP, AH, X509.3, CEP, IKE, Diffie-Hellman key exchange, 3DES, MD5

Applicable Internet Engineering Task Force (IETF) Request-for-Comments (RFC) includes all current RFCs related to the technology elements and modules previously listed.

APPLICABLE FORMS: None.

PROCEDURES:

General Information:

The objectives of the **gateway to gateway multi-node VPN standard** are to:

Protect State of Michigan internal systems from unauthorized use.

Increase the level of trust inherent in the State of Michigan network infrastructure.

Support the secure data transfer needs of the State's agencies workforce, business partners, and small remote offices for 24 x 7 access to internal system hosted resources from host networks not operated or managed by the State of Michigan.

Prevent alteration, destruction, or modification of data system information.

Prevent disclosure of information classified as protected under state statute to unauthorized individuals.

Benefits expected:

Accommodate appropriate use of low-cost access to state resources over the Internet or business partner networks.

Increased security for internal hosts and networks.

Reduction of risks associated with use of Internet or extra-net "public" networks.

Maintain acceptable levels of network management efficiency.

Accrue cost savings from use of public network connections when appropriate for workers not housed at State of Michigan owned or leased facilities.

Easier maintenance and enforcement of enterprise level security policies.

Opportunity to integrate Quality of Service (QOS) practices.

Applicability:

Conditions of Application:

This standard applies to non-browser client connections from desktops, laptops, or workstations, servers or hosts that require access to any internal State of Michigan host system, server, or network connected host device. It specifically is applicable when the network, host, or device contains information that is classified as protected under Michigan compiled laws, and the connection is carried over networks that are not managed by or specifically for the State of Michigan.

All routes redirected for the hosts or client users while attached as traversing the State of Michigan's home gateway VPN node concentrators will be directed and limited to internal hosts on the LMAN or SOM-WAN exclusively.

This standard applies to extra-net access. Extra-net is defined as any State of Michigan to business partner Internet tunneled or direct connection or value added network connection where one or more connecting clients or hosts are outside of the State of Michigan's network and the internal destination host is on any of the State of Michigan's internal host networks.

This standard applies to Internet client or host access. Internet is defined as any State of Michigan employee, contractor, or partner connection across the public Internet, VPN tunneled, or Internet Service Provider access or through any Access Service Provider where one or more connecting nodes or clients are outside of the State of Michigan trusted network perimeter and the internal destination host is on any of the State of Michigan's internal host networks.

This standard does not cover:

1. Host connections internal to the State of Michigan trusted perimeter networks (LMAN or SOM-WAN).
2. Secure Sockets Layer (SSL) enabled client Web browser applications available to the Internet.
3. Intermittent connections made over the public switched telephone network using a plain old telephone (POTS) or integrated services digital network (ISDN) dial-in-connections to the State of Michigan's central modem bank.
4. This standard does not address the total security access needs and is intended to supplement and/or be combined with other security standards and best practices when indicated as necessary to provide adequate risk reduction.

Assumptions:

- Agency remote hosts are accessing State of Michigan network and server resources with state agency provided equipment or host servers configured, managed, and maintained by agency technical staff. Where employees gain access to State of Michigan network and server resources with personal privately owned equipment, only SSL enabled web browser applications available to the Internet are employed for access.
- Further that these web browser enabled applications should utilize application layer security best practices such as user name and password, and/or pin number combinations at a minimum, to reduce risk of unauthorized access leading to inappropriate use.

In addition to use of VPN technology, agency network or host administrators shall provide appropriate security though best practices applicable to application level, network, or host operating system security.

Implementation considerations:

This standard applies when the remote connections are for more than one client, server, or host device and the connection is for random intermittent time periods that can occur frequently each day. Connections from remote locations that require or place a steady average demand for bandwidth at or above thresholds generally available over public

networks or are running applications that require low-data-transmission-latencies should become a routed node directly connected on the LMAN or SOM-WAN. SOM-WAN connection may be a preferred alternative to use of VPN technology over unreliable networks.

Agencies must coordinate specific remote access needs with the Network Operations Center (NOC) and review security risk threat profile analysis with the Enterprise Security Director.

DMB will deploy VPN concentrators to provide IPsec enabled VPN tunnels on the Internet and/or Extra-net connection points to State of Michigan networks. The concentrators will use hardware encryption. Issuance of keys for the 3DES (3DES encryption) and Internet Key Exchange (IKE) negotiated encryption will require a written request to the Network Operations Center (NOC) from the agency security administrator. The Network Operations Center administrator will maintain appropriate logs and documents pertaining to issuance of keys. Agencies shall establish internal procedures to immediately notify NOC when VPN tunnels should be withdrawn from access control and security association lists maintained by NOC.

Agencies may not, under any circumstances, establish any VPNs tunneled across public networks that are not terminated on DMB concentrators and managed by NOC. Management and operation of all VPNs security associations with a node external to the trusted network perimeter must be handled by the NOC and approved by the Enterprise Security Director.

Technical

Considerations: Implementations of multi-node VPN will standardize on pairs of IPSec-enabled gateways with security associations configured for using both Encapsulating Security Payload (ESP) and Authentication Header (AH) support, a tunnel mode security association and pre-shared or dynamically assigned keys to provide 3DES (168 bit) encryption. Along with 3DES encryption use of the MD5 hashing algorithm is mandatory to provide en-route data integrity. Personal authentication when required for individual client connections will be provided by two-factor authentication currently provided by Securid cards. Issue of Securid cards are authorized by the agency security administrators signed letter to the Network Operation Center. All VPN connections will link to the enterprise concentrator before being routed through the State of Michigan firewall and switched connections to internal networks.

Additional data encapsulation through the use of lower security (under 128 bit) encryption algorithms on the host device or client before passing the data packets to the gateway, where desirable and technically possible, to provide added host application security is not disallowed by this standard. Tunneling of non-IP protocol packets within secure IPSec-IP-packets is also not disallowed by this standard, but must be done by hosts or appliances, not on the gateways.

Maintenance:

DMB: Acquisition Services shall not approve any acquisition or purchase requests without confirmation from the Department of Information Technology, Office of Strategic Policy that such request is in compliance with the standard.

Operational Units (OU): Any and all projects, consulting requests, equipment and software acquisition requests, or ITB's relating to external gateway to gateway VPNs will be subject to review for compliance with this standard.

DIT: The Office of Strategic Policy will review this standard on a continuing basis and make recommendations for changes. An appropriate group of staff, representing a wide-range of state operational units, will review and possibly revise these standards and guidelines as often as needed.

Exceptions from this standard for reasons other than those outlined above will be made through the exception handling process described in the Exception Process Template.
